A Personnel/User Database Implementing EAR/ITAR-Compliant Access Controls to a Project Information System[1]

Robin Dumas and Donna Avila
Jet Propulsion Laboratory
4800 Oak Grove Drive
Pasadena, CA 91109
818-354-8512 and 818-354-3805
rdumas@sirtfweb.jpl.nasa.gov and davila@sirtfweb.jpl.nasa.gov

Keevin Fisher
Raytheon ITSS
299 N. Euclid
Pasadena, CA 91101
626-744-5429
kfisher@sirtfweb.jpl.nasa.gov

Abstract—As the National Aeronautics and Space Administration (NASA) continues to implement geographically and internationally diverse project teams, the necessity of controlling access to shared information causes increasing concern among team members and requires strict implementation of processes and procedures. The complexity of sharing information among such project teams when partners are not collocated has created a need to obtain and validate user credentials. In addition, NASA's missions are increasingly lower-cost and have shorter design and development cycles, forcing cost constraints on information system implementation and maintenance.

The Jet Propulsion Laboratory (JPL), as a Federally Funded Research and Development Center (FFRDC) under contract to NASA, must comply with all Federal statutes and regulations applicable to import and export control. Specific controls include the Export Administration Regulations (EAR) [1], International Traffic in Arms Regulations (ITAR) [2] [3], and the Code of Federal Regulations (CFR) [2][3][4], which apply to dissemination of information. Implementing EAR- and ITAR-compliance in a complex information system environment with stringent cost constraints dictates a simple, cost-effective implementation that is easily modifiable for a variety of projects.

NASA's Space Infrared Telescope Facility (SIRTF) project recently developed and implemented a combined EAR/ ITAR-compliant access request and project personnel database at its JPL project office. SIRTF's implementation of a web-based interface to the database provides access requests, access approval, user account creation and validation, and a project telephone list. NASA's Galaxy Evolution Explorer (GALEX), a low-cost SMEX mission adapted SIRTF's prototype at virtually no cost, proving the portability of the SIRTF solution.

This paper describes the approach used in designing the SIRTF prototype, describes the difficulties encountered, and explains the adaptability of the database to varying levels of project complexity.

1. Introduction

The SIRTF personnel/user database evolved from the SIRTF project secretary's Excel spreadsheet. When the project was still in Pre-Phase A and under development, the SIRTF project secretary created a spreadsheet to keep track of project personnel. This spreadsheet tracked name, phone number, company, and instrument or system for each individual assigned to the project. This was a simple solution that worked well when the project was small. As SIRTF moved from Pre-Phase A to Phase A, the number of project personnel began increasing. SIRTF was estimated to include less than 1000 personnel at peak times.

Simultaneously, the SIRTF system administrator was implementing a web-based project archive/library that would later develop into its project information system and creating a user access control system. Initially each user account was created when a SIRTF manager requested it. These user accounts were created not only for personnel located at JPL and Caltech, but also for SIRTF's geographically diverse industry and university partners.

It was decided that the telephone directory and the user access control system could be combined into one access control and display mechanism. How to establish and implement the system became the next obstacle. Since

[1] 0-7803-7231-X/01/$10.00/ © 2002 IEEE

SIRTF uses a web interface for its project information system, a web-based solution was evaluated. The geographically diverse locations of the SIRTF partnering institutions added to the reasons for implementing a web-based solution. Utilizing a web interface also meant that the solution would be independent of applications and processes already in use by the SIRTF partners.

2. Establishing a Personnel/User Database

Although initially a spreadsheet was adequate for keeping track of project personnel and contact information, it became clear that the spreadsheet was no longer adequate. The decision on when to establish a personnel database may vary from project to project, but a simple solution is to create it from the beginning of the project and have the controls and procedures already in place. Anytime the user list gets too big for one person to easily update, or if it is being updated weekly or daily, it is time to implement a user database.

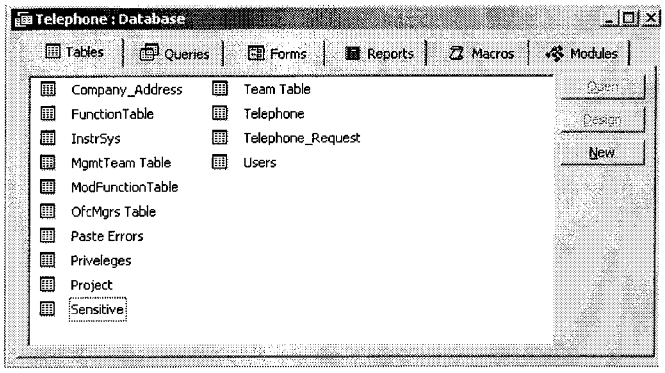
The project secretary and the system administrator decided to create a relational database that would serve as an access request mechanism as well as a means of collecting and distributing project personnel contact information. They decided to implement a web-based interface to the database. Because this interface was via the web, access as well as maintenance and accuracy of information contained in the database was distributed to all project partners—each maintaining their portion of the database.

By using a relational database rather than a spreadsheet, information such as company addresses could be handled automatically by the database without users having to enter the information. Therefore, the information is more accurate as individual entries and the associated chances for typographical errors are eliminated. Another upside was that updating one occurrence in the company address table changes all occurrences for that company in the telephone table.

In addition, the web interface was created to authenticate usernames using of the NT user accounts, thereby allowing permissions for modifications to the database to be set and changes to the database to be tracked by username, implementing an ISO 9000-compliant [5] environment. Each addition and change to the database is tracked in the database, but only the most current information is reflected in the web interface. The historical record of changes helps meet ISO 9000 standards.

Database Design

Design of the database is important in establishing connections between users, permissions, as well as affiliations including company and instrument. Tables must be created that capture these relationships. Before designing the database, relationships between various bits of information must be explored and parent-child relationships determined. Figure 1 shows the table design for the SIRTF Telephone/Access Database.


Telephone : Database

Company_Address
FunctionTable
InstrSys
MgmtTeam Table
ModFunctionTable
OfcMgrs Table
Paste Errors
Priveleges
Project
Sensitive
Team Table
Telephone
Telephone_Request
Users

Figure 1. SIRTF personnel/user database tables

Controlling User Access to the System

As with any process implementation, cost is a factor to consider. In NASA's *faster*, *better*, *cheaper* environment, any tools developed must be necessarily simple, easy to use, and cost effective to develop and implement. In addition, because of the sensitive nature of ITAR controls, user access must be controlled not only through processes, but in most cases user access privileges should be invisible to the user. That is, the user should be able to see what he has permission to see and not gain access to information he does not have permission to see.

Therefore, in the NASA environment any user access control system should offer the necessary level of security and must include:

- Simplicity – simple to learn, easy to use
- Flexibility – can be easily modified to meet requirements of any project
- Extensibility – can be refined and enhanced for more complex applications
- Repeatability – can be used for a variety of project sizes and cost constraints
- Support – cost of support must be minimal

3. Implementing EAR and ITAR Compliance

Since EAR and ITAR regulations require both JPL's and SIRTF's compliance, any access control system that is implemented must establish controls that address these regulations and must establish the necessary compliance. Implementing an EAR- and ITAR-compliant system is as much determining a process that follows organizational policies and procedures as well as it is a physical control mechanism. In order to assure EAR and ITAR compliance the process must be documented and the procedures must be followed.

In this case, SIRTF decided to create three classifications: *ITAR Approved*, *ITAR Restricted*, and *ITAR Waived* as part of its access control process. *ITAR Approved* is the classification assigned to all U.S. citizens including those with green cards. *ITAR Restricted* is the classification assigned to all foreign nationals who have not been granted an access license by the State Department. *ITAR Waived* is the classification assigned to all foreign nationals who have been granted limited access according to their State Department license.

Only the general ITAR classifications as listed above are tracked by the database—details of individual licenses are maintained separately according to JPL policies. At JPL, details of State Department licensing and accesses by foreign nationals are handled by JPL's International Affairs and the project follows their policies and procedures for tracking foreign national access. A physical copy of licenses is maintained separately from the database.

The process created for SIRTF access control and ITAR-compliance is relatively simple. Users may request access through the *User Request Form* as shown in Figure 2 as well as via phone or email. The account information is then verified before the account is created and information added to the database. This process is described in more detail under the section *User Access Controls and Procedures.*

2. USER ACCESS RECOMMENDATIONS

The following recommendations are made for ease of establishing an access control system. Recommendations are necessarily platform independent and should comply with any institutional computer security regulations. SIRTF follows JPL Computer Security guidelines. [6] [7] [8] [9]

Users and Groups

Users—a unique account is created for each user according to their assigned ITAR approval level. Detailed information on user accounts is given in the section *User Access Controls and Procedures.* User accounts are not to be shared, nor are passwords to be used by anyone other than the user. Each user is responsible for maintaining the integrity of their user account and password. Any account suspected of being compromised is immediately disabled, and the user is notified. Any account not accessed for 120 days may be deleted.

Main Groups

It is recommenced that two main groups be created. One main group is for all personnel who are not foreign nationals. This group has access to all information in the system. Foreign Nationals are assigned to a second group, referred to as the *lite* group. The *lite* group has access only to information considered in the public domain (not restricted or already approved for release) such as information on the public web site, meeting information, the telephone directory, etc. An example of the two main groups in the SIRTF system is indicated in Table 1.

Table 1. Sample of Groups used by SIRTF project.

Group	**Description of Users**
Main Groups	
STARS	All *ITAR Approved Users*
STARSlite	All *ITAR Restricted* or *ITAR Waived* users
Subgroups	
Project	JPL Project Managers Only
SDT	SIRTF Design Team Only

Subgroups

Additional groups are created as needed. Each project should determine their requirements for subgroups and create groups and group assignments accordingly. By using subgroups permissions can be assigned to the group level, rather than the individual user level. A sample of the SIRTF subgroups is shown in Table 1.

Foreign Nationals

All foreign nationals should be designated as restricted access by default and should be given access only to the information that has been approved and specified according to the State Department license and to your institutional policies and procedures. Access should not be given to any foreign national until such approval is received.

3. SUGGESTED USER ACCESS CONTROLS AND PROCEDURES

General User Accounts

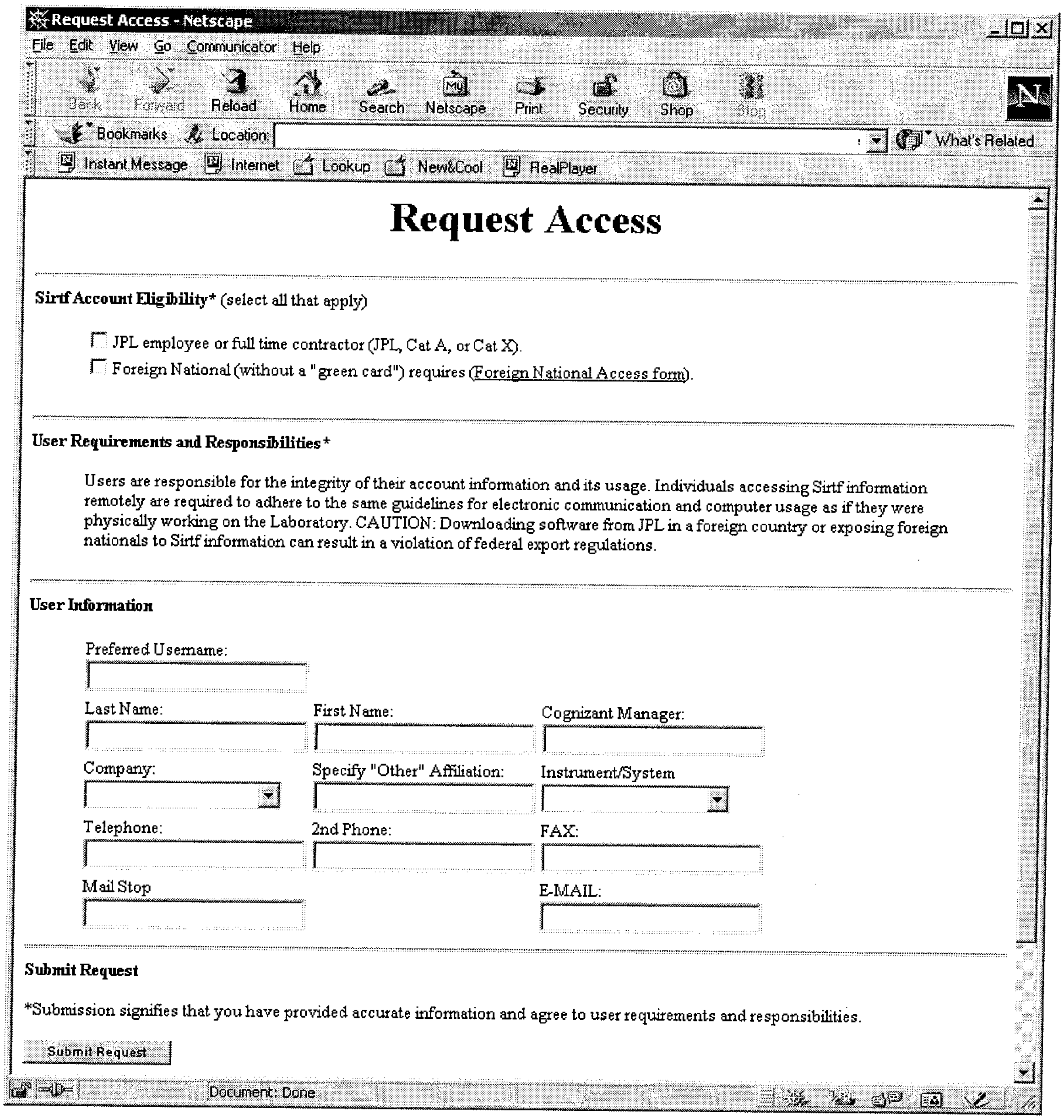
General user accounts should be established only upon completion of a *Request Access* form such as the one shown in Figure 2. In the SIRTF system the form must be filled out completely and is not be processed if information is not provided for the Cognizant Manager, Instrument/System, User Name, Phone Number, and Email Address and whether or not the user is a foreign national. In the SIRTF system, if a user is not a foreign national, the user is marked as *ITAR Approved.*

Once the form is completed and submitted, it gets placed into a pending queue where it should be reviewed and the information provided should be verified. Once reviewed and verified, the request is approved and the information is added to the database.

Foreign National User Accounts

Foreign National user accounts are processed much the same as general user accounts with the exception of checking the *Foreign National* box. Checking this box marks the user as *ITAR Restricted.* This means the user account is created with restricted access as a *lite* group member.

Because the user has checked the *Foreign National* box, access to restricted information should not given until the


Request Access - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: What's Related
Instant Message Internet Lookup New&Cool RealPlayer
Document: Done

Request Access

Sirtf Account Eligibility* (select all that apply)

□ JPL employee or full time contractor (JPL, Cat A, or Cat X).
□ Foreign National (without a "green card") requires (Foreign National Access form).

User Requirements and Responsibilities*

Users are responsible for the integrity of their account information and its usage. Individuals accessing Sirtf information remotely are required to adhere to the same guidelines for electronic communication and computer usage as if they were physically working on the Laboratory. CAUTION: Downloading software from JPL in a foreign country or exposing foreign nationals to Sirtf information can result in a violation of federal export regulations.

User Information

Preferred Username:

Last Name: First Name: Cognizant Manager:

Company: Specify "Other" Affiliation: Instrument/System

Telephone: 2nd Phone: FAX:

Mail Stop E-MAIL:

Submit Request

*Submission signifies that you have provided accurate information and agree to user requirements and responsibilities.

Submit Request

Figure 2. SIRTF access request form available via web interface on project web site.

State Department license is issued and clearance has been given for the individual to gain access to restricted information. The user should then be marked as *ITAR Waived*, meaning the user has access to information included in the license.

In general, Foreign Nationals have access only to meeting information, the telephone directory, the image archive, as well as other information cleared for release to the general public. All other information in the system, particularly a project archive or library is restricted to foreign nationals.

Retiring User Accounts

Although many projects have processes for adding user accounts, retiring user accounts is often overlooked. Upon leaving the project, user accounts should be disabled for 90 days and then deleted. Accounts may not be automatically deleted in the event that personnel may return to the project or require access during a phase out of their workload. User accounts should be reconciled at least once a year and all retired accounts should be removed from the system.

Password Procedures/Account Lockout

It is recommended that passwords be set to expire every 90 days and only be reestablished upon contact and verification by a system administrator. Ninety days is the current estimate for the time it would take a cracking program to compromise passwords. However, policies regarding IT security for your institution should be followed. In addition to password expiration, failed attempts to access an account should be considered. In general it is recommended that five failed attempts to access any account should result in that account being locked out until an administrator is notified.

4. Personnel Telephone Directory

The web interface to the SIRTF Personnel Telephone Directory provides easy access to the database. The default user interface displays the telephone directory in the left frame and the search capability in the right frame as shown in Figure 3.

Each column of the telephone directory provides a clickable sort function—clicking on the title for the column sorts the database in ascending order according to that column. This is achieved through the ASP code used in the web interface.

In addition, the user has the ability to either add a new entry or request addition of a new entry depending upon user privileges set in the database. Each user is given permission to modify only his entry. A designated group administrator at each of the partnering institutions is given permission to update and delete entries for that institution. The database administrator is given permission to update or remove all entries.

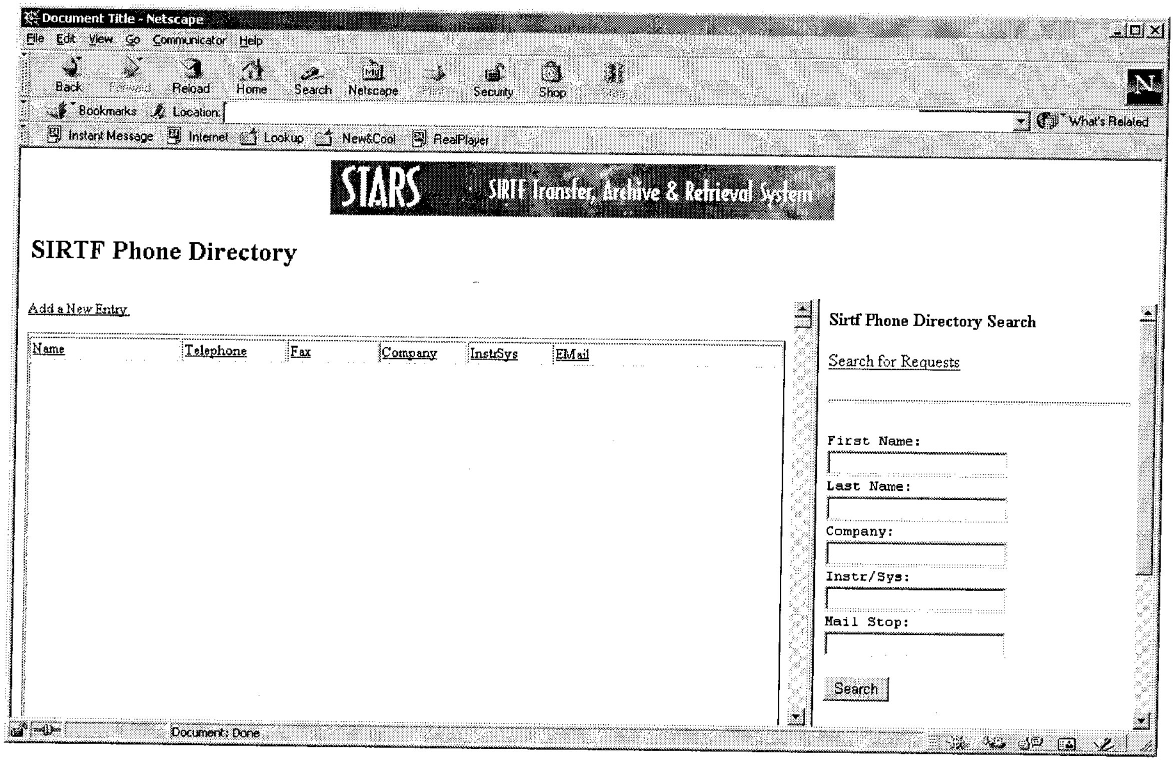
The search capability allows users to search by first name, last name, company, instrument/system, or mail stop. This provides an easy interface to creating a listing for each partnering institution. It also makes it easy for the user to find someone even knowing only partial information. Administrators are given permission to search for requests, which takes them to the approval process for each account.

5. Probems Encountered

Several problems were encountered during the development of the personnel/user database system. This section discusses these problems and resolutions.

The first problem encountered concerns when to establish a database and was discussed in the section *Establishing a Personnel/User Database*. The next problem encountered was which application should be used. SIRTF chose to use Microsoft Access as it was already using that application. Any SQL database application can be used, and your choice should consider which application is being used by your institution.

A series of decisions regarding the design of the database and the control of access brought to light some communication problems with partnering institutions. SIRTF found that different institutions used different terminology and common terminology was developed so that all partners understood and communicated about the same thing. Something as simple as whether to refer to it as the telephone directory or telephone list encouraged discussions.



SIRTF Phone Directory

Add a New Entry

Name	Telephone	Fax	Company	InstrSys	EMail

Sirtf Phone Directory Search

Search for Requests

First Name:

Last Name:

Company:

Instr/Sys:

Mail Stop:

Search

Figure 3. SIRTF Phone Directory via web interface.

The design of the database including which tables to include and what relationships between the tables should exist formed the next series of problems to be solved.

Perhaps one of the biggest obstacles to overcome when implementing and EAR- and ITAR-compliant system is to find out which regulations apply to your institution and which policies and procedures you must follow. It is also important to consider institutional organization of information technology in any of your decisions. Daniels, who says, "IT applications must be prioritized in line with strategic objectives", reinforces this. [10]

Another thing to consider is that if you are creating a process you must document the process. Although many people create systems, processes, and procedures, it is often more difficult to get people to document what they have done, and why certain decisions were made in order to facilitate extensibility and repeatability.

6. ADAPTABILITY

The section *Establishing a Personnel/User Database* mentions that any access control system must include: Simplicity, Flexibility, Extensibility, Repeatability, and Support. In order for a system to be easily adaptable, it must include these features.

A database, almost by definition, is considered adaptable as what is included can be easily tailored to the particular need. In the case of a personnel/user database different projects will probably require different information or additional information. For example, when the database was ported from SIRTF to GALEX, GALEX decided it needed to have job descriptions. Making this addition required adding a field to the database and including it in the web interface. Modifying the SIRTF database for GALEX also proved repeatability as well as extensibility.

7. CONCLUSIONS

Implementing any EAR- and ITAR-compliant system necessitates creating processes that follow policies and procedures of your institution, as much as it necessitates creating a physical system.

Research described in this paper was performed at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

REFERENCES

[1] *Export Administration Regulations (EAR)*, 15 CFR chapter VII, subchapter C. [Online]. Available: http://w3.access.gpo.gov/bxa/index.html (Sept. 2001).

[2] 22CFR125, Code of Federal Regulations, Title 22, Volume 1, Chapter 1, Part 120. Revised as of April 1, 2001. U.S. Government Printing Office via GPO Access. [Online] Available: http://www.access.gpo.gov/nara/cfr/waisidx_01/22cfr120_01.html

[3] 22CFR125, Code of Federal Regulations, Title 22, Volume 1, Chapter 1, Part 125. Revised as of April 1, 2001. U.S. Government Printing Office via GPO Access. [Online] Available: http://www.access.gpo.gov/nara/cfr/waisidx_01/22cfr125_01.html

[4] 22CFR9, Code of Federal Regulations, Title 22, Volume 1, Chapter 1, Part 9. Revised as of April 1, 2001. U.S. Government Printing Office via GPO Access. [Online] Available: http://www.access.gpo.gov/nara/cfr/waisidx_01/22cfr9_01.html

[5] ISO 9000. [Online] Available: http://www.iso.ch/iso/en/ISOOnline.frontpage (Sept. 2001).

[6] *JPL Information Technology Security Requirements for Computer Users*, JPL D-7223, Rev. 5. Pasadena, CA: Jet Propulsion Laboratory (2001).

[7] *JPL Information Technology Security Requirements for Computer Systems*, JPL D-7155, Rev. 3. Pasadena, CA: Jet Propulsion Laboratory (2000).

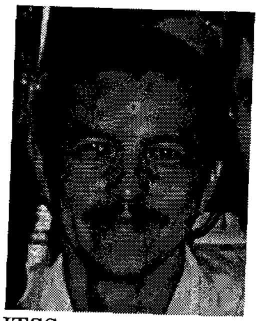
[8] *NPD 2810. Security of Information Technology* (1998). [Online] Available: http://nodis3.gsfc.nasa.gov/library/displayDir.cfm?Internal_ID=N_PD_2810_0001_&page_name=main (Sept. 2001).

[9] *NPG 2810, NASA Procedures and Guidance for the Security of Information Technology*, (1999). [Online] Available: http://nodis3.gsfc.nasa.gov/library/displayDir.cfm?Internal_ID=N_PG_2810_0001_&page_name=main (Sept. 2001).

[10] N. Caroline Daniels, *Information Technology: The Management Challenge,* Boston: Pearson Custom Publishing, 2000.

Robin Dumas is a senior information systems engineer at the Jet Propulsion Laboratory. She currently works as the Information Technology Manager for the SIRTF and GALEX projects at JPL. She is also a Contract Work Order Manager for the Project Information Enterprise Resources at JPL. She is responsible for designing, implementing, and maintaining the project informa-tion systems. She is also respon-sible for implementing and maintaining a collaborative meeting environment that connects geographically diverse project partnering institutions. Her information technology fields of expertise include web applications, databases, information management technology, and knowledge management. She is currently participating in research in the fields of asteroid astrometry and infrared astronomy. She has an AA degree from Pasadena City College and is currently completing a BSIT degree.

Donna Avila is the SIRTF Project Documentarian and Configuration Management Administrator. Her responsibilities as project documentarian include maintaining project documents and records, and designing web pages for the project information system. In her previous position as project secretary she first had the idea to move the project telephone list to a database and subsequently designed the database.



Keevin Fisher is currently working as a Manager of the Project Information Enterprise Resources Group at Raytheon ITSS in Pasadena. His areas of technical expertise include database design, programming, information management technologies, and knowledge management. His is currently responsible for overseeing the Raytheon ITSS contract for the group. He is currently working on his BSIT degree.